

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-261914

(43)Date of publication of application : 13.09.2002

(51)Int.Cl.

H04M 1/66

H04Q 7/38

H04L 9/32

H04M 11/00

(21)Application number : 2001-060195

(71)Applicant : HITACHI LTD

(22)Date of filing : 05.03.2001

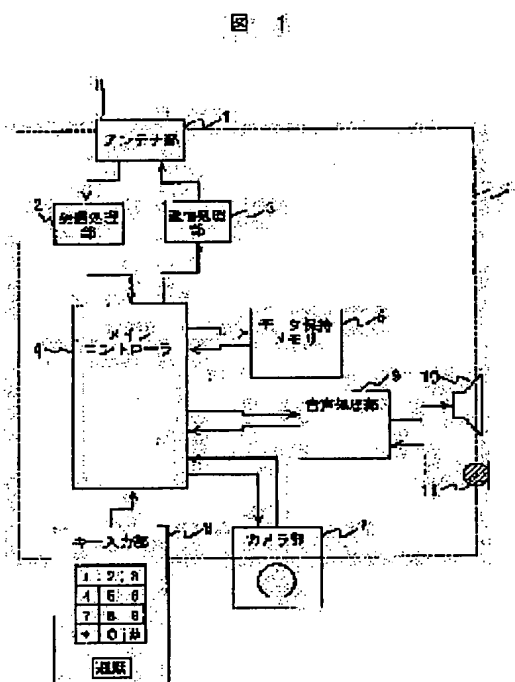
(72)Inventor : OBATA SHINICHI
MATSUDA MASAYUKI
SHINAGAWA AKIO

(54) PORTABLE COMMUNICATION TERMINAL HAVING USER CERTIFICATION FUNCTION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a portable communication terminal having a user certification function, which can trace an illegal user.

SOLUTION: The portable communication terminal having a user certification function for certifying a user by comparing image data whose image is picked up in response to operation start with data for comparison being stored in advance has a means for transmitting image data whose image has been picked up to the outside and to continuing communication operation when the comparison does not match.



LEGAL STATUS

[Date of request for examination] 22.02.2005

[Date of sending the examiner's decision of rejection] 24.04.2007

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-261914

(P2002-261914A)

(43) 公開日 平成14年9月13日 (2002.9.13)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 M 1/66		H 0 4 M 1/66	5 J 1 0 4
H 0 4 Q 7/38		11/00	3 0 2 5 K 0 2 7
H 0 4 L 9/32		H 0 4 B 7/26	1 0 9 R 5 K 0 6 7
H 0 4 M 11/00	3 0 2	H 0 4 L 9/00	6 7 3 D 5 K 1 0 1

審査請求 未請求 請求項の数 5 O L (全 8 頁)

(21) 出願番号 特願2001-60195(P2001-60195)

(22) 出願日 平成13年3月5日 (2001.3.5)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 小畑 信一

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内

(72) 発明者 松田 雅之

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内

(74) 代理人 100068504

弁理士 小川 勝男 (外2名)

最終頁に続く

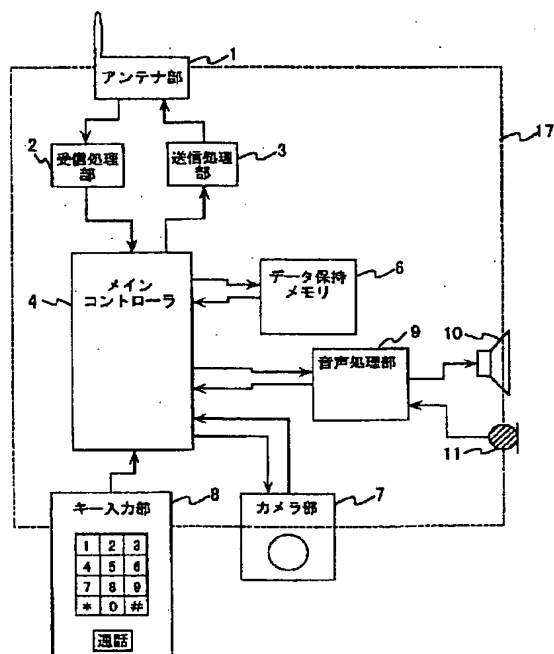
(54) 【発明の名称】 使用者認証機能付き携帯通信端末

(57) 【要約】

【課題】不正使用者の逆探知が可能な使用者認証機能付き携帯通信端末を提供する。

【解決手段】操作開始に応答して撮像した画像データを、予め記憶の照合用データと照合して、使用者の認証を行う使用者認証機能付き携帯通信端末において、前記照合が一致しない場合に、前記撮像した画像データを外部に送信し且つ通信動作を継続させる手段を備えたことを特徴とする。

図 1



【特許請求の範囲】

【請求項 1】操作開始にตอบสนองして撮像した画像データを、予め記憶の照合用データと照合して、使用者の認証を行う使用者認証機能付き携帯通信端末において、前記照合が一致しない場合に、前記撮像した画像データを外部に送信し且つ通信動作を継続させる手段を備えたことを特徴とする使用者認証機能付き携帯通信端末。

【請求項 2】操作キーの押圧にตอบสนองして撮像した画像データを、予め記憶の照合用データと照合して、使用者の認証を行う使用者認証機能付き携帯通信端末において、前記押圧した操作キーの種類に応じて前記予め記憶の照合用データの種類の切り替え、前記撮像した画像データを前記撮像した画像データに対応した照合用データと照合して使用者の認証を行う手段と、前記照合が一致しない場合に、前記撮像した画像データを外部に送信し且つ通信動作を継続させる手段を備えたことを特徴とする使用者認証機能付き携帯通信端末。

【請求項 3】請求項 1 記載の使用者認証機能付き携帯通信端末において、前記撮像した画像データが顔画像データであり、前記予め記憶の照合用データが照合用顔画像データであり、前記手段は、前記顔画像データを前記照合用顔画像データと照合し、前記照合が一致しない場合に、前記撮像した顔画像データを外部に送信し且つ通信動作を継続させることを特徴とする使用者認証機能付き携帯通信端末。

【請求項 4】請求項 1 記載の使用者認証機能付き携帯通信端末において、前記撮像した画像データが外耳画像データであり、前記予め記憶の照合用データが照合用外耳画像データであり、前記手段は、前記外耳画像データを前記照合用外耳画像データと照合し、前記照合が一致しない場合に、前記撮像した外耳画像データを外部に送信し且つ通信動作を継続することを特徴とする使用者認証機能付き携帯通信端末。

【請求項 5】請求項 2 記載の使用者認証機能付き携帯通信端末において、前記操作キーが通話キーとそれ以外のキーからなり、前記予め記憶の照合用データが照合用顔画像データと照合用外耳画像データからなり、前記手段は、前記押圧した操作キーが前記通話キーの場合に前記撮像した画像データを前記照合用外耳画像データと照合して使用者の認証を行い、前記押圧した操作キーが前記通話キー以外のキー場合には前記撮像した画像データを前記照合用顔画像データと照合して使用者の認証を行うことを特徴とする使用者認証機能付き携帯通信端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯通信端末に関し、特に、使用者を認証する機能を有する使用者認証機能付き携帯通信端末に関する。

【0002】

る従来の認証システムは、例えば、特開 2000-30028 号公報に記載されているような、指紋、声紋、網膜紋等の一致を確認するものである。そのような認証システムでは、適正使用者の指紋、声紋、網膜紋を照合用パターンとして予め登録しておき、その保持された照合用パターンと、外部から入力されたパターンとを比較することで認証処理を実現している。

【0003】

【発明が解決しようとする課題】特開 2000-30028 号公報のような認証システムにおいては、照合用パターンを予め登録しておくため、ある決まった一個人を特定するに足る情報を電子的な形態で保持することになる。本来、指紋、声紋、網膜紋などは、本人が有する唯一無二の身体的特徴と考えられており、本人の体以外には存在しないという点で、様々な分野において個人特定的手段として、大きな威力を発揮してきた。

【0004】しかし、その特徴を示す情報を照合用パターンとして電子的な形態で保持することにより、かえって、その照合用の情報が乱用される危険性が新たに生じる。その場合、特に指紋、網膜紋、DNA パターン等などは、それ自体が確実に一個人を特定するため、乱用されたことを主張することは著しく困難となる。また、複数人数で携帯電話等を共用する場合などは、その使用者管理においては、指紋、網膜紋ほどの厳密さは必要なくとも、不正使用者については、しっかりとチェックされる必要がある。

【0005】本発明の目的は、不正使用者の逆探知が可能な使用者認証機能付き携帯通信端末を提供することにある。

【0006】本発明の他の目的は、操作キーの種類により予め記憶の照合用データが切り替えられ且つ不正使用者の逆探知が可能な使用者認証機能付き携帯通信端末を提供することにある。

【0007】

【課題を解決するための手段】本発明は、操作開始にตอบสนองして撮像した画像データを、予め記憶の照合用データと照合して、使用者の認証を行う使用者認証機能付き携帯通信端末において、前記照合が一致しない場合に、前記撮像した画像データを外部に送信し且つ通信動作を継続させる手段を備えたことを特徴とする使用者認証機能付き携帯通信端末である。

【0008】本発明は、操作キーの押圧にตอบสนองして撮像した画像データを、予め記憶の照合用データと照合して、使用者の認証を行う使用者認証機能付き携帯通信端末において、前記押圧した操作キーの種類に応じて前記予め記憶の照合用データの種類の切り替え、前記撮像した画像データを前記撮像した画像データに対応した照合用データと照合して使用者の認証を行う手段と、前記照合が一致しない場合に、前記撮像した画像データを外部

特徴とする使用者認証機能付き携帯通信端末である。

【0009】本発明は、前記撮像した画像データが顔画像データであり、前記予め記憶の照合用データが照合用顔画像データであり、前記手段は、前記顔画像データを前記照合用顔画像データと照合し、前記照合が一致しない場合に、前記撮像した顔画像データを外部に送信し且つ通信動作を継続させることを特徴とする使用者認証機能付き携帯通信端末である。

【0010】本発明は、前記撮像した画像データが外耳画像データであり、前記予め記憶の照合用データが照合用外耳画像データであり、前記手段は、前記外耳画像データを前記照合用外耳画像データと照合し、前記照合が一致しない場合に、前記撮像した外耳画像データを外部に送信し且つ通信動作を継続することを特徴とする使用者認証機能付き携帯通信端末である。

【0011】本発明は、前記操作キーが通話キーとそれ以外のキーからなり、前記予め記憶の照合用データが照合用顔画像データと照合用外耳画像データからなり、前記手段は、前記押圧した操作キーが前記通話キーの場合に前記撮像した画像データを前記照合用外耳画像データと照合して使用者の認証を行い、前記押圧した操作キーが前記通話キー以外のキー場合には前記撮像した画像データを前記照合用顔画像データと照合して使用者の認証を行うことを特徴とする使用者認証機能付き携帯通信端末である。

【0012】

【発明の実施の形態】図1は、本発明の使用者認証機能付き携帯通信端末の実施の形態の構成図である。図1において、使用者認証機能付き携帯通信端末17は、無線通信用アンテナ部1と、無線通信用アンテナ部1からの受信信号を入力し復調処理をする受信処理部2と、送信用データを変調して無線通信用アンテナ部1に送る送信処理部3、メインコントローラ4と、照合用特徴データを保持するデータ保持メモリ6と、外部映像を撮像して画像データをメインコントローラ4に送るカメラ部7と、ユーザからのキー入力をデータ変換してメインコントローラ4に送るキー入力部8と、メインコントローラ4からの受信音声データを復号化処理し且つマイクからの音声入力を符号化処理する音声処理部9と、復号化処理された音声信号を受けて音を出すスピーカ10と、外部音声を取り込み音声信号とするマイク11とで構成されている。

【0013】次に、使用者認証の処理を説明すると、キー入力部8上のキーの押し下げがあったことをメインコントローラ4が検出し、カメラ部7に撮像指示が送信される。撮像指示を受けたカメラ部7は前面画像を撮像して、撮像データをメインコントローラ4に送る。メインコントローラ4では、比較対象領域を抽出し、比較対象領域内での特徴点の位置を特定して採取画像特徴データとする。更に採取画像特徴データとデータ保持メモリ6

内の照合用特徴データ群とを比較して、一致すると解釈される照合用特徴データがあるかどうか判断する。そこで、一致画像有りとなった場合は機能制限無しのフル機能モード設定にし、一致画像無しと判定された場合は機能制限された認証NG使用者用使用モード（使用制限モード）を設定にする。

【0014】更にメインコントローラ4では、認証NG使用者用使用モード（使用制限モード）が設定された場合、認証NGとなった使用者の送信画像データ124を、通信サービスセンタに送るために送信処理部3に出力する。送信処理部3はアンテナ部1を介して、通信サービスセンタに認証NGとなった使用者の送信画像データを送信する。

【0015】図2は、図1の使用者認証の処理の流れを示す処理フロー図である。処理スタート段階200に続き、キー押し下げ検出段階201により、電源キー、通話キー、テンキー等の入力キーが押し下げられたことを検出する。続いてキー押し下げが検出されたことを受け、前面画像撮影段階202において、携帯通信端末に搭載されたカメラ部により前面画像を撮像する。続いて比較対象領域輪郭検出段階203において、前面画像撮影段階202で撮像された採取画像データの中から比較対象領域を抽出する。続いて特徴パターン抽出段階204において、比較対象領域内での特徴パターンを抽出して採取画像特徴データとする。

【0016】続いて画像特徴ライブラリ検索段階205において、認証処理に使う照合用特徴データを呼び出す。続いて認証パターン照合判定段階207において、照合用特徴データの中に採取画像特徴データと一致すると解釈されるデータがあるかどうかを判定する。そこで、一致画像有り208となった場合は、続いて、フル機能モード設定段階212により、機能制限無しのフル機能モード設定にして、通信継続動作212に続く。

【0017】また、認証パターン照合判定段階207において一致画像無し209と判定された場合は、使用制限モード設定段階210により、機能制限された認証NG使用者用使用モード（使用制限モード）を設定にし、続いて、撮像画像データ送信段階211により、使用者の送信画像データを送信処理部3に送り、通信サービスセンタに認証NGとなった使用者の画像データを送信して、通信継続動作212に続く。

【0018】これにより、使用者の手を煩わせることなく、使用者認証処理が自動的に行われる。特に、その際に照合用データとして、指紋、網膜紋等の個人特定情報を電子的な形態で機器内に保持する必要が無くてすむため、個人特定情報を危険に晒す可能性を抑えることができる。さらに、使用者が不正使用者である場合でも続けて通信継続動作させ、その間に、不正使用者の逆探知が可能である。

【0019】逆探知の方法としては、採取された使用者

10

20

30

40

50

画像データを通信サービスセンタに送ることで、使用者の特徴がある程度判明する。また、携帯通信端末が現在使用している基地局の位置から、半径何m以内という範囲でおおよそ位置が特定できる。

【0020】図2において、比較対象領域を、使用者の顔画像とした場合には、図2における比較対象領域輪郭検出段階203が顔画像認識段階に代わり、特徴パターン抽出段階204が特徴抽出段階に代わり、画像特徴ライブラリ検索段階205が顔画像特徴ライブラリ検索段階に代わり、一致画像有り208が一致顔画像有り218に代わり、一致画像無し209が一致顔画像無し219に代わる。

【0021】これにより、使用者の顔画像を自動撮像して、簡易認証処理を行うことができる。また、認証用の照合用特徴データは顔画像の特徴を示すデータとなるため、万が一、乱用の危険性に晒された場合でも、指紋や網膜紋ほど被害が深刻なものにはならない。また、使用者が撮像装置に対して顔を背けている場合には、顔画像と認識されないため、認証NG使用者として判別できる。

【0022】この顔画像認識の例を示したのが、図3(a)～(d)である。図3(a)～(d)は、採取画像データ301、使用者顔画像302、比較対象画像領域303、第1特徴点304、第2特徴点305、第1特徴点X座標306、第1特徴点Y座標307とで構成されている。図3(a)は図2に示された前面画像撮影段階202において撮像された採取画像データである。続いて図3(b)は、図2に示された比較対象領域輪郭検出段階203に代わる顔画像認識段階において比較対象領域を抽出する様子を示している。

【0023】続いて図3(c)及び図3(b)は特徴パターン抽出段階204に代わる顔画像特徴抽出段階において顔画像内の特徴点を抽出する様子を示しており、右の目の位置となる第1特徴点304、右の頬のライン境界である第2特徴点305を初めとする複数の特徴点を丸で示している。続いて図3(d)は、特徴パターン抽出204に代わる顔画像特徴抽出段階において顔画像内の特徴点に関するパラメータデータを決定する様子を示しており、第1特徴点304に対するパラメータデータとして、第1特徴点X座標306と第1特徴点Y座標307を導出している。この特徴点座標306、307を照合用顔画像特徴データと比較することで、認証処理を行うことができる。

【0024】また、顔面画像による認証の例と同様に、図2の上記比較対象領域を、使用者の外耳画像とする例も考えられる。

【0025】その場合の外耳画像認識の例を示したのが、図4(a)～(d)である。図4(a)～(d)は、採取画像データ401、使用者外耳画像412、比較対象画像領域413、外耳の第1特徴点414、外耳

の第2特徴点415、外耳の第2特徴点X座標416、外耳の第2特徴点Y座標417とで構成されている。図4

(a)は図2に示された前面画像撮影段階202において撮像された採取画像データである。続いて図4(b)は、図2に示された比較対象領域輪郭検出段階203において比較対象領域413を抽出する様子を示している。

【0026】続いて図4(c)及び図4(b)は特徴パターン抽出段階204において外耳画像内の特徴点を抽出する様子を示しており、第1特徴点414、第2特徴点415を初めとする複数の特徴点を丸で示している。続いて図4(d)は、特徴パターン抽出段階204において外耳画像内の特徴点に関するパラメータデータを決定する様子を示しており、外耳の第2特徴点415に対するパラメータデータとして、外耳の第2特徴点X座標416と外耳の第2特徴点Y座標417を導出している。この特徴点座標416、417を照合用外耳画像特徴データと比較することで、認証処理を行うことができる。

【0027】ここで、図7に、実際の携帯通信端末の一例である携帯電話機を使っている使用者の様子を示した。携帯電話機は、使用者70、使用者の耳71、携帯電話機72、スピーカ73、カメラ部(撮像装置)74、表示画面75、入力キー部76、マイク77とで構成されている。図7に示したとおり携帯電話機を使った通常通話時の場合には、その使用時間の大半において携帯電話機のそばにあるのは耳である。従って、外耳の画像を認証に利用するのは大変便利である。また、顔画像同様、外耳画像では一個人を特定するほどの厳密な情報とはならないので、その利用、管理も危険性が低い。

【0028】次に、使用者認証の他の処理を説明する。この処理フローは、押し下げキーの種類により、照合用の特徴データの種類の切り替えるものである。これは、使用している用途により、携帯通信端末の正面に位置する使用者の顔の部分異なることに着目した機能である。すなわち、通常通話機能使用時では、携帯通信端末には使用者の耳が近接したままになり、Webサイトブラウジング等の時は、使用者は表示画面が顔の正面になるように携帯通信端末を持つことが想定されるので、その切り替えを、押し下げキーの種類で行うようにしたものである。

【0029】図1において、キー入力部8上のキーの押し下げがあったことをメインコントローラ4が検出し、カメラ部7に撮像指示が送信される。撮像指示を受けたカメラ部7は前面画像を撮像して、撮像データをメインコントローラ4に送る。メインコントローラ4では、比較対象領域を抽出し、比較対象領域内での特徴点の位置を特定して採取画像特徴データとする。

【0030】ここで、押し下げがあったキー入力部8上のキーが通話キーであるか、それ以外(テンキー、特殊

記号キー) であるかをメインコントローラ 4 が判別する。押し下げがあったキーが通話キーであった場合には、メインコントローラ 4 が照合用特徴データ群の種類を外耳特徴データ群と設定して、押し下げがあったキーが通話キー以外のキーであった場合には、メインコントローラ 4 が照合用特徴データ群の種類を顔面特徴データ群として設定する。

【0031】更に採取画像特徴データとデータ保持メモリ 6 内の設定された照合用特徴データ群とを比較して、一致すると解釈される照合用特徴データがあるかどうか判断する。

【0032】図 5 は、この使用者認証の他の処理の流れを示す処理フロー図である。処理スタート段階 200 に続き、キー押し下げ検出段階 201 により、電源キー、通話キー、テンキー等の入力キーが押し下げられたことを検出する。続いて押し下げキー判別段階 220 により、押されたキーが通話キーかどうか判定される。押し下げられたキーが通話キーの場合には、通話開始時撮像段階 221 により、通話開始時点で撮像する。続いて外耳画像照合用特徴データ比較段階 222 において、通話開始時撮像段階 221 での撮像データに対して、照合用外耳画像特徴データとの比較を行う。

【0033】押し下げキー判別段階 220 により、押し下げられたキーが通話キーでない場合には、画像撮像段階 223 において前面画像を撮像し、顔面画像照合用特徴データ比較段階 224 において、前面画像データに対して、顔面画像照合用特徴データとの比較を行う。

【0034】続いて認証パターン照合判定段階 207 において、照合用特徴データの中に採取画像特徴データと一致すると解釈されるデータがあるかどうかを判定する。そこで、一致画像有りとなった場合は、続いて、フル機能モード設定段階 212 により、機能制限無しのフル機能モード設定にして、継続動作 212 に続く。また、認証パターン照合判定段階 207 において一致画像無しと判定された場合は、使用制限モード設定段階 210 により、機能制限された認証 NG 使用者用使用モード (使用制限モード) を設定にし、続いて、撮像画像データ送信段階 211 により、使用者の送信画像データを送信処理部に送り、通信サービスセンタに認証 NG となった使用者の画像データを送信して、継続動作 212 に続く。

【0035】これにより、使用者の手を煩わせることなく、使用者認証処理が自動的に行われる。また、その際に照合用データとして、指紋、網膜紋等の個人特定情報を電子的な形態で機器内に保持することが無いため、個人特定情報を危険に晒す可能性を抑えることができる。更に、使用状況に応じて、比較認証用の対象画像の種類

を自動的に切り替えることができる。

【0036】ここで、照合用画像特徴データの例と、認証 NG 時の送信画像データの例を、図 6 (a)、(b) に示す。図 6 (a) は照合用画像特徴データテーブル 620 を示しており、ユーザ ID 621 と、使用機能履歴データ 622 と、照合用特徴パラメータデータ 623 とで構成されている。これによりユーザ別の照合用特徴パラメータデータが管理され、認証処理に利用することができる。また、図 6 (b) は認証 NG となった使用者の送信画像データテーブル 624 を示しており、端末 ID 625 と、使用機能履歴データ 622 と、採取画像データ 626 とで構成されている。これにより認証 NG となった使用者に関する画像を機器の外部に伝えることができる。

【0037】これにより、使用者の手を煩わせることなく、使用者認証処理が自動的に行われる。また、その際に照合用データとして、指紋、網膜紋等の個人特定情報を電子的な形態で機器内に保持することが無いため、個人特定情報を危険に晒す可能性を抑えることができる。さらに、使用者が不正使用者である場合でも続けて継続動作させるので、その間に、不正使用者の逆探知が可能である。

【0038】

【発明の効果】本発明によれば、不正使用者の逆探知が可能な使用者認証機能付き携帯通信端末を提供することができる。また本発明によれば操作キーの種類により予め記憶の照合用データが切り替えられ且つ不正使用者の逆探知が可能な使用者認証機能付き携帯通信端末を提供することができる。

【図面の簡単な説明】

【図 1】本発明の使用者認証機能付き携帯通信端末の実施の形態の構成図である。

【図 2】図 1 の使用者認証の処理の流れを示す処理フロー図である。

【図 3】顔面画像認識の例を示した図である。

【図 4】外耳画像認識の例を示した図である。

【図 5】使用者認証の他の処理の流れを示す処理フロー図である。

【図 6】照合用画像特徴データの例と、認証 NG 時の送信画像データの例を示す図である。

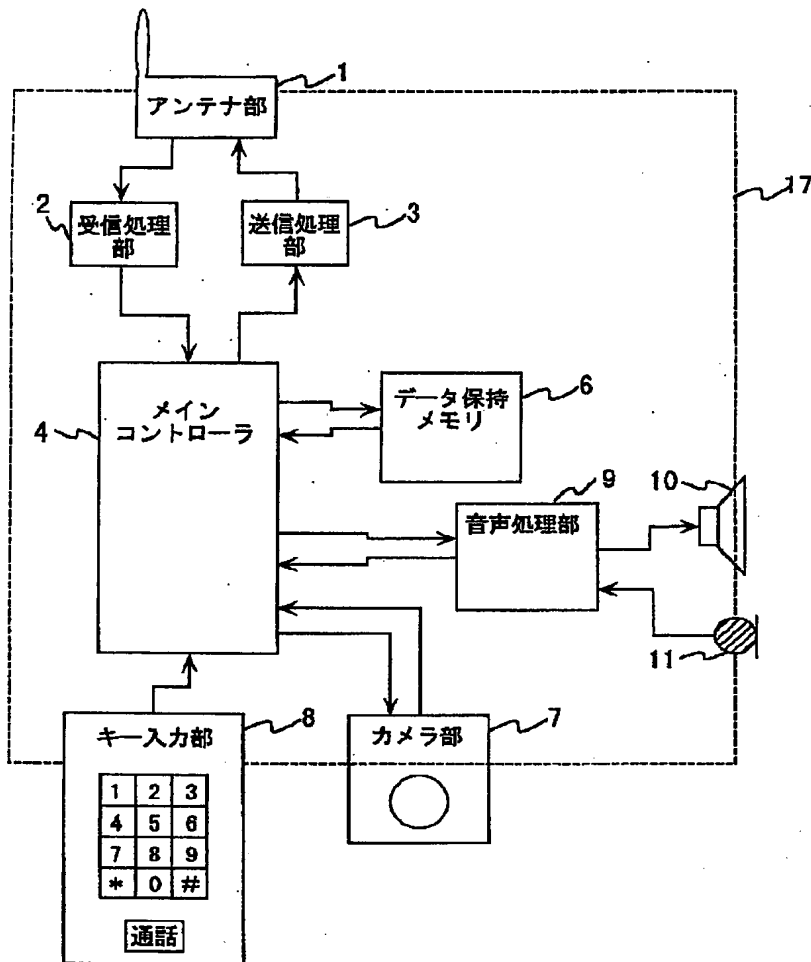
【図 7】実際の携帯通信端末の一例である携帯電話機を使っている使用者の様子を示した図である。

【符号の説明】

1…アンテナ部、2…受信処理部、3…送信処理部、4…メインコントローラ、6…データ保持メモリ、7…カメラ部、8…キー入力部、9…音声処理部、10…スピーカ、11…マイク。

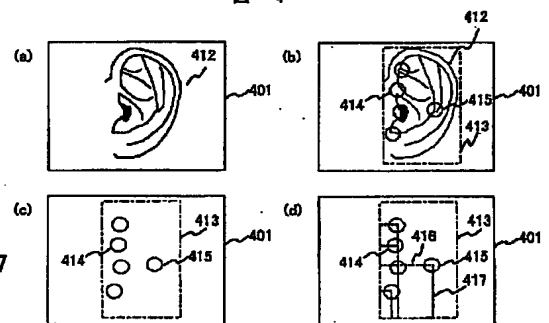
【図1】

図 1



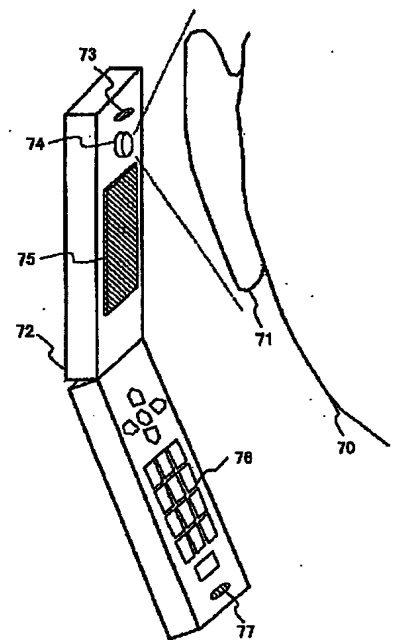
【図4】

図 4



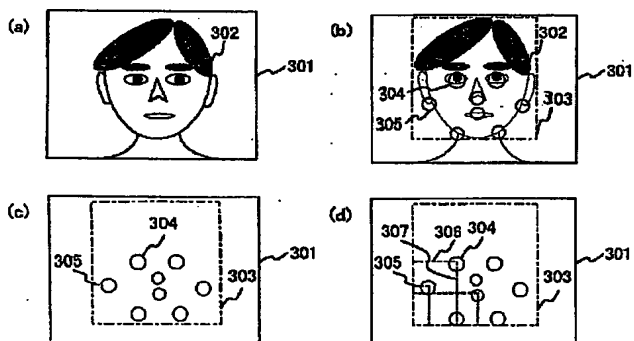
【図7】

図 7



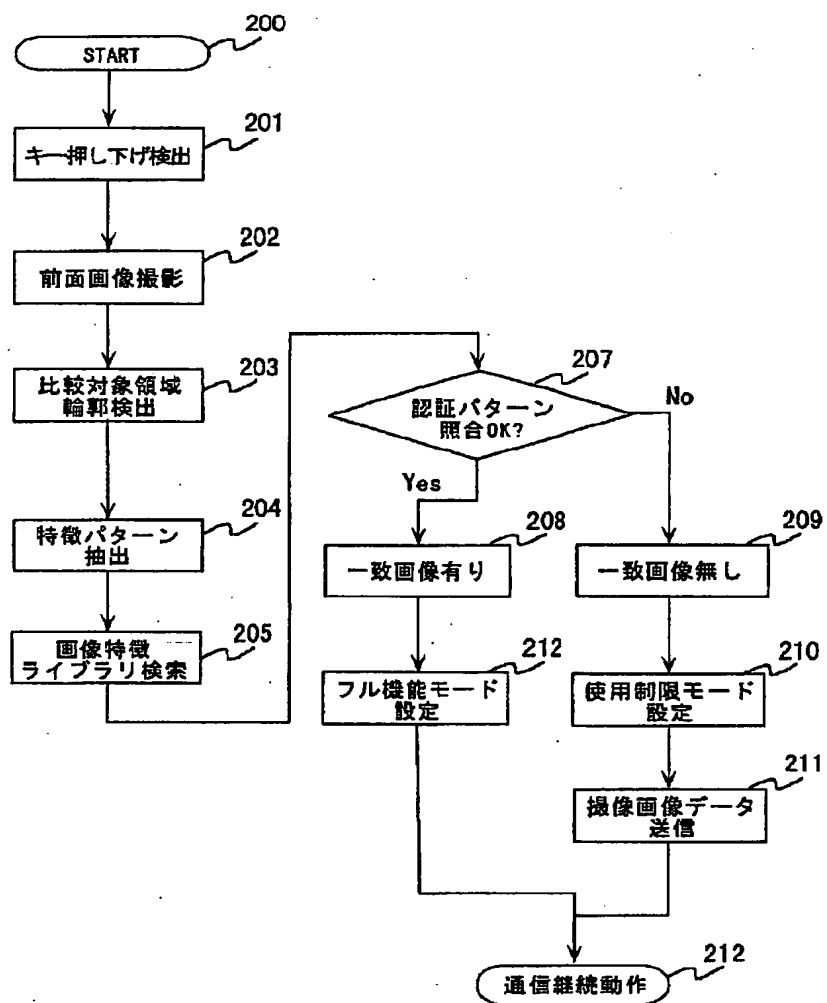
【図3】

図 3



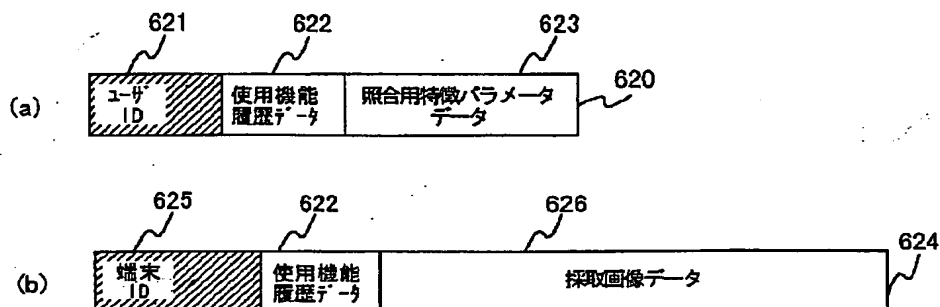
【図2】

図 2



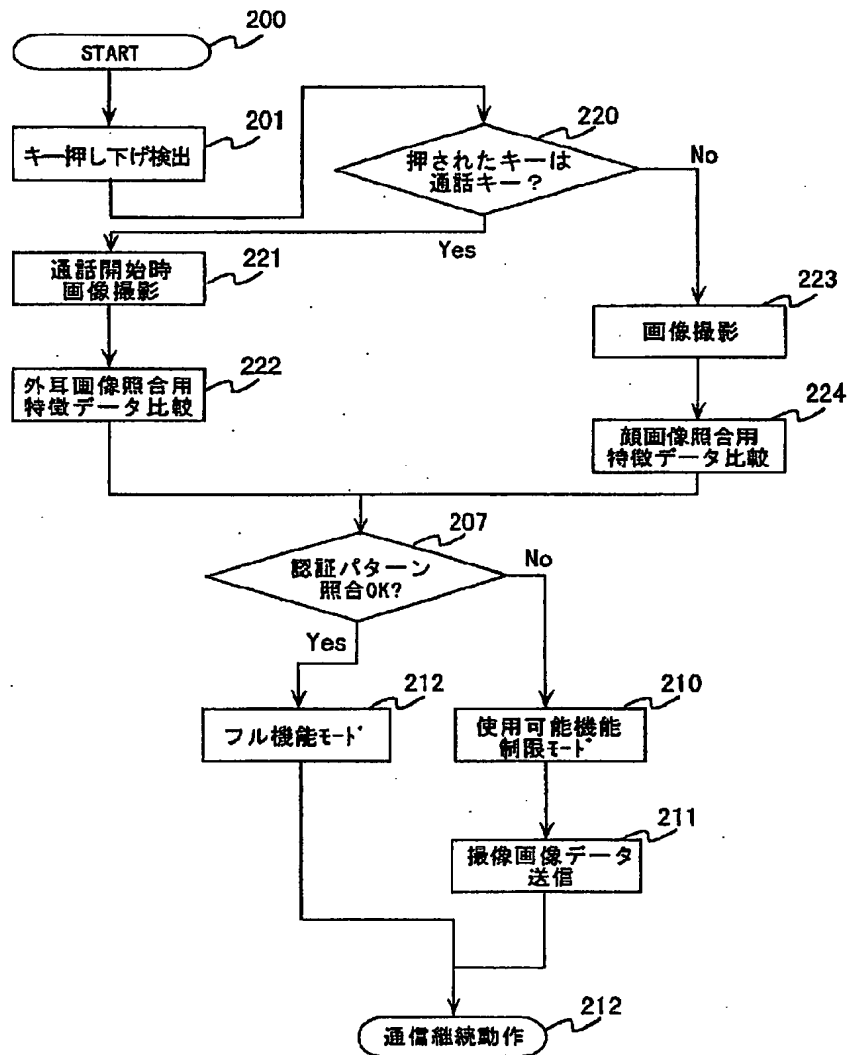
【図6】

図 6



【図5】

図 5



フロントページの続き

(72)発明者 品川 明生
茨城県ひたちなか市稲田1410番地 株式会
社日立製作所デジタルメディア製品事業部
内

Fターム(参考) 5J104 AA07 AA12 KA01 KA16 PA02
5K027 AA11 BB09 HH11 HH23 HH29
5K067 AA32 DD17 DD52 EE02 GG01
HH22 HH23
5K101 LL12 NN06 PP03